IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ALISTAIR STEWART, individually and on behalf of all others similarly situated Plaintiff, v. ADVOCATE AURORA HEALTH, INC. and META PLATFORMS, INC., Defendants.	Case No. 1:22-cv-5964 JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, Alistair Stewart ("Plaintiff"), individually on behalf of himself and on behalf of all others similarly situated, by and through undersigned counsel, brings this Class Action Complaint against Defendants Advocate Aurora Health, Inc. ("Advocate") and Meta Platforms, Inc. ("Facebook"), and alleges as follows:

NATURE OF THE ACTION

1. This is a medical privacy action against Advocate and Facebook, for violating the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510, *et seq.*, violating the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, and violating other privacy rights by knowingly and repeatedly intercepting, accessing, and disclosing the personally identifiable, sensitive and confidential statutorily-protected patient health information (PHI) of Advocate's patients without their knowledge, authorization, or consent.

2. Healthcare providers such as Advocate have a strict fiduciary duty to keep patient data, communications, diagnoses, treatment information, and other PHI completely confidential unless authorized to make disclosures by the patient.

3. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996), and the implementing regulations of the United States Department of Health and Services ("HHS") establish a national standard to protect patient health care information, medical records, and other individually identifiable information.

4. HHS provides guidance for healthcare providers that patient status alone is protected by HIPAA.

5. Accordingly, patients of Advocate have a reasonable expectation of privacy that the content of their communications with Advocate, including diagnoses, treatment information, personally identifiable information, and PHI, will not be intercepted, transmitted, re-directed, or disclosed by Advocate or Facebook without the patient's knowledge, authorization, or consent.

6. Like many other hospitals and healthcare providers, Advocate encourages patients to use its supposedly "secure" patient online MyChart portal (branded as "LiveWell" to patients) to communicate with Advocate, including, but not limited to, to communicate with doctors, request prescription refills, access test results, view their account details, schedule appointments, make payments, and access their doctor's notes.

7. Whenever a patient uses Advocate's websites and applications, including its LiveWell portal, Advocate and Facebook intercept, contemporaneously cause transmission of, and use personally identifiable patient information and PHI without patients' knowledge, consent, or authorization.

8. Advocate and Facebook collect and shares the personally identifiable information and PHI of patients using a "Meta Pixel." A Meta Pixel is a snippet of programming code that, once installed on a webpage or mobile application, tracks users – unbeknownst to them – as they

navigate through a website or application and transmits information regarding the user's activity to Facebook.

9. On October 20, 2022, Advocate confirmed its violations when it posted a "Notice of Data Breach" on its website, publicly disclosing for the first time that "[w]hen using some Advocate Aurora Health sites, certain protected health information ("PHI") would be disclosed in particular circumstances to specific vendors because of pixels on our websites or applications."[1] Based on Advocate's investigation, the following sensitive patient information may have been involved: patient IP addresses; dates, times, and/or locations of scheduled appointments; patients' proximity to an Advocate location; information about patients' medical providers; type of appointment or procedure; communications between patients and others through MyChart, which may have included first and last names and medical record numbers; information about whether patients had insurance; and, if patients had a proxy MyChart account, the patient's first name and the first name of their proxy.

10. Advocate discloses its patients' personally identifiable patient information and PHI to Facebook together in a single transmission. This transmission occurs even though patients have not shared (nor consented to share) such information.

11. As a consequence of Advocate and Facebook's conduct in knowingly and repeatedly intercepting, accessing, and disclosing personally identifiable patient information and PHI without patient knowledge, consent, or authorization, Advocate has violated the ECPA; breached and betrayed the confidential nature of the healthcare provider-patient relationship; and removed the private nature of sensitive and confidential information that Plaintiff and Class

[1] *See* https://www.advocateaurorahealth.org/pixel-notification/.

members intended to remain private. Facebook, moreover, has violated the ECPA, SCA, and breached its own contractual promises made to its users.

12. Advocate and Facebook disregarded the statutorily protected and common law privacy rights of Plaintiff and thousands of other patients. Accordingly, Plaintiff brings this class action for legal and equitable remedies to redress and put a stop to Advocate and Facebook's practice of intercepting and disclosing personally identifiable patient information and other PHI.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*. and the Stored Communications Act, 18 U.S.C. § 2701, *et seq*.

14. This Court also has jurisdiction under 28 U.S.C. § 1332(d) because this action is a class action in which the aggregate amount in controversy for the proposed Class (defined below) exceeds $5,000,000, and at least one member of the Class is a citizen of a state different from that of either Defendant.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendants do business in and are subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claim occurred in or emanated from this District.

THE PARTIES

16. Plaintiff Alistair Stewart is a natural person and a citizen of the State of Illinois. Plaintiff has been a patient of Advocate since at least 2018 and a LiveWell patient portal user and user of Facebook since at least 2018. During the relevant time period, Plaintiff has visited Advocate's websites to schedule appointments, view test results, access his doctor's notes,

message doctors and nurses, and review medications. By doing so, Plaintiff's personally identifiable patient information and PHI was intercepted and disclosed by Advocate and Facebook under the systematic process described herein. Plaintiff had no knowledge that his sensitive medical information was shared with Facebook or other third parties and gave no consent or authorization for Advocate to disclose his personally identifiable patient information and PHI.

17. Defendant Advocate is a non-profit health care corporation with dual headquarters in Milwaukee, Wisconsin and Downers Grove, Illinois. Advocate encourages patients, which number in the thousands, to use and communicate with medical providers through the Advocate LiveWell patient portal. The Advocate Children's Hospital, Aurora Health Care, Advocate Cancer Institute, Advocate Heart Institute, Advocate Brain and Spine Institute, and Orthopedic Center, are all a part of Advocate.

18. Defendant Facebook is a Delaware corporation and multinational technology conglomerate with its principal place of business in Menlo Park, California.

FACTUAL BACKGROUND

I. Advocate Aurora Health's LiveWell Patient Portal

19. Advocate maintains the LiveWell patient portal for its patients to communicate with Advocate, including but not limited to exchanging communications about bill payments, doctors, services, test results, and appointments.[2]

20. In April 2018, Advocate Health Care in Illinois merged with Aurora Health Care in Wisconsin. The LiveWell patient portal (formerly the MyAdvocateAurora portal) was created as a combined patient portal experience.[3]

[2] *See* https://www.advocateaurorahealth.org/livewell/faq.
[3] *Id.*

21. Advocate's patient portal, www.livewell.aah.org/chart, or "LiveWell", allows its patients to communicate with Advocate with options including but not limited to "message your doctor," "manage your appointments," and "handle your family's health."[4]

22. Plaintiff communicated with LiveWell, identified himself to Advocate as a patient, and exchanged messages with his medical providers about medical conditions.

23. Advocate states that its LiveWell portal "makes it easier than ever to manage your health and access the care you need,"[5] and that "the LiveWell with Advocate Aurora Health app and website are secure environments."[6]

24. Advocate's privacy policy purports that it supports and recognizes its "patients' right to expect that their medical records and other information about their care will be kept confidential."[7]

25. Notwithstanding these promises, Advocate deployed Facebook's Meta Pixel and other third-party web beacons and tracking pixels on LiveWell that cause the contemporaneous unauthorized transmission of personally identifiable patient information and PHI and the precise content of patient communications with LiveWell to Facebook whenever a patient uses LiveWell's patient portal.

II. Facebook's Contractual Promises

26. Anytime a person, including Plaintiff, initiates a Facebook account, they legally agree to its Terms, Data Policy, and Cookie Policy via a checkbox on the sign-up page. These Terms, Data, and Cookie Policies are binding upon Facebook and its users.

[4] *See* https://www.advocateaurorahealth.org/livewell/.
[5] *See* https://www.advocateaurorahealth.org/livewell/faq#what-is-livewell.
[6] *See* https://www.advocateaurorahealth.org/livewell/faq#security-sign-in.
[7] *See* https://www.advocatehealth.com/privacy-policy/.

27. The Facebook Data Policy expressly states that Facebook "requires" businesses that use the Meta Pixel "to have lawful rights to collect, use, and share your data before providing any data to [Facebook]."[8]

28. However, Facebook does not verify that the businesses using Meta Pixel have obtained the requisite consent as stated in their Data Policy.

29. Instead, Facebook applies an "honor system" where businesses "represent[s] and warrant[s] that [they have] provided robust and sufficient prominent notice to users regarding the Business Tool Data collection, sharing, and usage."[9]

30. As a result, the Meta Pixel is made available to any willing business or publisher regardless of the nature of their business.

31. Facebook's Meta Pixel contracts with healthcare providers such as Advocate fail to mention or comply with HIPAA.

III. Types of Personally Identifiable Patient Information and PHI that Advocate and Facebook Intercept and Transmit

32. Personally identifiable patient information and PHI that Advocate and Facebook intercept and transmit whenever a patient uses Advocate's website or application includes, but is not limited to, patient IP addresses; dates, times, and/or locations of scheduled appointments; patients' proximity to an Advocate location; information about patients' medical providers; type of appointment or procedure; communications between patients and others through MyChart, which may have included first and last names and medical record numbers; information about whether patients had insurance; and, if patients had a proxy MyChart account, the patient's first name and the first name of their proxy.

[8] *See* https://www.facebook.com/privacy/policy/version/20220104/.
[9] *See* https://www.facebook.com/legal/terms/businesstools.

IV. How Advocate and Facebook Intercept and Disclose Patients' Personally Identifiable Information and PHI

A. Tracking Pixels

33. The Facebook Meta Pixel, also known as a "tag" or "web beacon" among other names, is an invisible tool that tracks consumers' actions on Facebook advertisers' websites and reports them to Facebook. It is a version of the social plugin that gets "rendered" with code from Facebook. To obtain the code for the Pixel, the website owner tells Facebook which website events it wants to track (*e.g.*, scheduling an appointment or messaging a doctor) and Facebook returns corresponding Meta Pixel code for the advertiser to incorporate into its website.

34. Facebook benefits from websites like Advocate installing its Meta Pixel. When the Pixel is installed on a business's website, the business has a greater incentive to advertise through Facebook or other Meta-owned platforms, like Instagram. In addition, even if the business does not advertise with Facebook, the Pixel assists Facebook in building more fulsome profiles of its own users, which in turn allows Facebook to profit from providing more (and more lucrative) targeted ads. The Pixel is installed on websites all over the internet and, accordingly, provides Facebook with information about its users' preferences, other distinguishing traits, and web-browsing activities outside of Meta-owned platforms.

35. Advocate installed the Meta Pixel, which enabled Advocate and Facebook to intercept and disclose Plaintiff's and Class Members' personally identifiable patient information and PHI, because it benefits financially from the targeted advertising and information services that stem from use of the Pixel. When an Advocate patient uses LiveWell to schedule an appointment, view test results, view their doctor's notes, or conducts any action, the website or application sends certain information about the patient to Facebook, including, but not limited to, their identity and

the specific actions they took and health procedures they underwent. As such, Advocate and Facebook intercept and disclose sensitive and personally identifiable patient information and PHI.

B. Facebook ID ("FID")

36. An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. When a Facebook user, such as Plaintiff, with one or more personally identifiable FID cookies on their browser uses Advocate's LiveWell portal, Advocate, through its website code, causes the patient's identity and personally identifiable patient information and PHI to be transmitted to Facebook by the user's browser. This transmission is not the patient's decision, but results from Advocate and Facebook's purposeful use of the Meta Pixel by incorporation of that Pixel and code into Advocate's LiveWell portal. Advocate and Facebook could easily program LiveWell or the Meta Pixel so that this information is not automatically transmitted to Facebook when a patient logs in and uses the portal. However, it is not in either Defendant's financial interest to do so because they both benefits financially by providing this highly sought-after information.

37. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile, and with only the FID and the sensitive PHI that Advocate and Facebook knowingly, readily, and repeatedly intercept and disclose without any consent from the patients, connect the identity of the Facebook user profile with the types of medical procedures the patient underwent, and even access the patient's doctor's notes from Advocate.

38. At all relevant times, Advocate and Facebook knew that the Meta Pixel intercepted and disclosed personally identifiable patient information and PHI. This was evidenced from, among other things, the functionality of the Pixel, including that it enabled Advocate's LiveWell portal to show targeted advertising to its digital subscribers based on the products those digital subscribers had previously viewed on the website, including certain medical tests or procedures, for which Advocate received financial remuneration.

V. Advocate Admitted that it Unlawfully Disclosed its Patients' Personally Identifiable Patient Information and PHI to Facebook.

39. Advocate maintains a vast digital database comprised of its patients' personally identifiable patient information and PHI which in its October 20, 2022 "Notice of Data Breach," Advocate admitted to transmitting to certain third-party vendors, including Facebook.

40. Advocate did not share anonymized, non-personally identifiable data with Facebook. To the contrary, the data it disclosed is tied to unique identifiers that track specific Facebook users. Advocate has thus monetized its database by disclosing its patients' PHI to Facebook in a manner which allows Facebook to make a direct connection to patients' personal identities – without the consent of its patients and to the detriment of their legally protected privacy and medical rights.

41. Critically, the personally identifiable patient information and PHI Advocate disclosed to Facebook allowed for Facebook to build out its trove of personally identifiable data by cross-referencing and adding to the data it already has in its own detailed user profiles.

42. As a result of Advocate's data compiling and sharing practices, Advocate knowingly disclosed to Facebook (for its own personal profit) the personally identifiable patient information and PHI of its patients.

43. Advocate did not seek its patients' prior written consent for the disclosure of their personally identifiable patient information and PHI (in writing or otherwise), and until Advocate voluntarily provided public notice of its practices, its patients remained unaware that their PHI and other sensitive data was disclosed to Facebook.

44. By disclosing its patients' personally identifiable patient information and PHI to Facebook – which undeniably reveals their identity and other sensitive medical data – Advocate has intentionally and knowingly violated the ECPA. And by knowingly intercepting this data, Facebook has likewise intentionally and knowingly violated the ECPA.

VI. Plaintiff's Experience

45. Plaintiff Alistair Stewart has been a patient of Advocate since at least 2018. Plaintiff has been a LiveWell patient portal user since at least 2018.

46. When Plaintiff became a patient of Advocate and used the LiveWell patient portal, he provided his name, date of birth, zip code, and any cookies associated.

47. Plaintiff has had a Facebook account since at least 2012. From at least 2018 to the present, Plaintiff has used Advocate web properties to schedule appointments, view test results, access his doctor's notes, message doctors and nurses, and review medications.

48. Plaintiff never consented, agreed, authorized, or otherwise permitted Advocate to disclose his personally identifiable patient information and PHI to Facebook. Plaintiff was never provided written notice that Advocate discloses his personally identifiable patient information and PHI. Patient was never provided any means of opting out of the disclosure of his personally identifiable patient information and PHI. Nonetheless, Advocate knowingly disclosed Plaintiff's personally identifiable patient information and PHI to Facebook.

49. Because Plaintiff is entitled by law to privacy in his electronic communications with Advocate through the LiveWell patient portal, Advocate and Facebook's intentional interception and disclosure of his communications constitutes as a deprivation of the full set of benefits to which he is entitled.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action individually and on behalf of all others similarly situated as a class action under Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of the following class (the "Class"):

> All persons in the United States who are, or were patients of Advocate Aurora Health, or any of its affiliates, and accessed a patient portal that caused a transmission of personally identifiable patient information, PHI, and other electronic communications to be made to Facebook.

51. This action is properly maintained as a class action under Federal Rules of Civil Procedure 23(a) because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. The claims of the Plaintiff are typical of the claims of the class; and,

D. The Plaintiff will fairly and adequately protect the interests of the class.

Numerosity

52. Members of the Class are so numerous and geographically dispersed that joinder of all members of the Class is impracticable. Plaintiff believes that there are thousands of members of the Class. Class members can be identified from Advocate's records and Facebook's records.

Typicality

53. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been

harmed by Advocate's and Facebook's failure to comply with the ECPA, Facebook's failure to comply with the SCA, and violations other common law privacy and contractual rights. The common questions of law and fact include, but are not limited to the following:

A. Whether Advocate had a duty to protect and refrain from disclosing Plaintiff's and Class members' personally identifiable patient information and PHI;

B. Whether Advocate knowingly disclosed Plaintiff's and Class members' personally identifiable patient information and PHI to Facebook;

C. Whether Facebook knowingly intercepted Plaintiff's and the Class members' personally identifiable patient information and PHI;

D. Whether Plaintiff and Class members authorized or consented to Advocate's disclosure of their personally identifiable patient information and PHI to Facebook;

E. Whether the information disclosed to Facebook concerning Plaintiff's and Class members' personally identifiable patient information and PHI constitutes unlawful interception of electronic communication under the ECPA;

F. Whether Advocate and Facebook's interception and disclosure of Plaintiff's and Class members' personally identifiable patient information and PHI was intentional under the ECPA;

G. Whether the Facebook's Terms, Data Policy, and Cookie Policy are valid contracts and whether Facebook breached those contracts;

H. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' conduct.

54. Plaintiff anticipates that Advocate and Facebook will raise defenses that are common to the class.

Adequacy

55. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and the class members. Plaintiff,

moreover, has retained experienced counsel that are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

56. Plaintiff's claims are typical of the claims of members of the Class. Plaintiff and members of the Class were harmed by the same wrongful conduct by Advocate and Facebook that caused personally identifiable patient information and PHI to be intercepted and disclosed without obtaining express written consent. Plaintiff's claims are based on the same legal theories as the claims of other Class members.

Predominance and Superiority

57. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

58. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Advocate and Facebook

and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

FIRST CAUSE OF ACTION

Violation of the Electronic Communications Act ("ECPA"), 18 U.S.C. § 2510, *et seq.*
Advocate and Facebook Defendants

59. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

60. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any … electronic communication" or "intentionally discloses, or endeavors to disclose, to any person the contents of any … electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] … electronic communication" or "intentionally uses, or endeavors to use, the contents of any … electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] … electronic communication." 18 U.S.C. §§2511 (1)(a), (c) – (d).

61. In addition, "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication [ ] while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511 (3)(a).

62. As defined in 18 U.S.C. § 2510 (12), "electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted

in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce."

63. As defined in 18 U.S.C § 2510(4), "intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."

64. As defined in 18 U.S.C § 2510(8), "contents" includes "any information relating to the substance, purport, or meaning" of the communication at issue.

65. As defined in 18 U.S.C § 2510(15), an "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications.

66. 18 U.S.C. §2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

67. Plaintiff and the Class members' use of Advocate's patient portal is an electronic communication under the ECPA.

68. Advocate's patient portal is an electronic communication service under the ECPA.

69. Whenever Plaintiff and Class members interacted with Advocate's patient portal, through the Meta Pixel it deployed and ran on its website, Advocate and Facebook contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiff's and Class members' electronic communications without authorization or consent.

70. Whenever Plaintiff and Class members interacted with Advocate's LiveWell portal, through the Meta Pixel it deployed and ran on its website, Advocate contemporaneously and intentionally disclosed, and endeavored to disclose the contents of Plaintiff's and Class members'

electronic communications to Facebook without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

71. Whenever Plaintiff and Class members interacted with Advocate's LiveWell portal, through the Meta Pixel it deployed and ran on its website, Advocate and Facebook contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and Class members' electronic communications, for purposes other than providing health care services to Plaintiff and Class members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

72. Whenever Plaintiff and Class members interacted with Advocate's LiveWell portal, through the Meta Pixel it deployed and ran on its website, Advocate and Facebook contemporaneously and intentionally redirected the contents of Plaintiff's and Class members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook.

73. Whenever Plaintiff and Class members interacted with Advocate's LiveWell portal, through the Meta Pixel it deployed and ran on its website, Advocate contemporaneously and intentionally divulged the contents of Plaintiff's and Class members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, including Facebook.

74. Advocate and Facebook intentionally intercepted and used the contents of Plaintiff's and Class members' electronic communications for the unauthorized purpose of disclosing and, profiting from, Plaintiff's and Class members' communications.

75. Plaintiff and Class members did not authorize Advocate or Facebook to acquire the content of their communications for purposes of sharing and selling the personally identifiable information and PHI contained therein.

76. Plaintiff, individually, on behalf of the Class members, seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages, punitive damages, preliminary and other equitable or declaratory relief, and attorneys' fees and costs.

SECOND CAUSE OF ACTION

Violation of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.* Facebook Defendant

77. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

78. A violation of the SCA occurs when anyone "intentionally accesses without authorization a facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a).

79. 18 U.S.C. § 2707(a) provides a private right of action to anyone "aggrieved by any violation" engaged in with a "knowing or intentional state of mind."

80. Advocate's LiveWell portal is a "facility" as defined by the SCA; the portal stores both the medical information of their users and the communications between Advocate and the Plaintiff and Class members.

81. Advocate allowed Facebook to access the personally identifiable patient information and PHI from its LiveWell portal through the deployment of the Meta Pixel.

82. Plaintiff and Class members did not have knowledge of, authorize, or consent to Facebook's accessibility to Plaintiff's and Class members' personally identifiable patient information and PHI stored in Advocate's LiveWell portal.

83. Facebook's access of Plaintiff's and Class members' personally identifiable patient information and PHI constitutes "unauthorized access" within the meaning of 18 U.S.C § 2701(a) because Plaintiff and Class members had no reasonable expectation their personally identifiable patient information and PHI would be shared with an unknown third party.

84. Facebook intentionally exceeded its authorization to access the Plaintiff's and Class members' personally identifiable patient information and other PHI through Advocate's LiveWell portal in violation of 18 U.S.C. § 2701(a)(2).

THIRD CAUSE OF ACTION

Breach of Contract
Facebook Defendant

85. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

86. Facebook requires users to click a box indicating that, "By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy."

87. "Click-wrap agreements" such as the one used by Facebook are valid and binding contracts.

88. The Facebook Terms, Facebook Data Policy, and Facebook Cookie Policy are binding on Facebook and its users.

89. The Facebook Data Policy promises users that Facebook "requires each of [Facebook's] partners to have lawful rights to collect, use and share your data before providing any data to [Facebook]."

90. Facebook breached this contractual promise, by not requiring its partners that are healthcare providers, including Advocate, to obtain patient consent before sharing patient status, patient portal communications, and other personally identifiable patient information and PHI with Facebook through the Meta Pixel.

91. Plaintiff and Class members are Facebook account holders who used Advocate's patient portals through which Facebook unlawfully obtained their personally identifiable patient information and other PHI.

92. The personally identifiable patient information and other PHI that Facebook obtained in breach of the contract include, but are not limited to:

a. Patient IP addresses;

b. Cookie identifiers;

c. Device identifiers;

d. Account numbers; and

e. Every electronic communication the patient has through the patient portals, including appointment scheduling, whether the patient viewed test results, patient communications with their doctors, and patient medical conditions.

FOURTH CAUSE OF ACTION

Breach of Implied Duty of Confidentiality
Advocate Defendant

93. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

94. Plaintiff and Class members were patients of the Advocate and received healthcare services from Advocate.

95. Advocate agreed to keep Plaintiff's and Class members' information confidential as part of establishing and maintaining the healthcare services provider/patient relationship between Advocate and the Plaintiff and Class members.

96. There is a duty of confidentiality implied in every healthcare provider and patient relationship, akin to an implied contract, such that healthcare services providers may not disclose

confidential information acquired through the healthcare provider-patient relationship. *See e.g.*, *Geisberger v. Willuhn*, 72 Ill. App. 3d 435, 438 (2d Dist. 1979).

97. The implied duty of confidentiality is at least as extensive as Advocate's statutory obligations as a healthcare services provider to maintain patient confidentiality.

98. Under the Illinois' Medical Patient Rights Act "health care provider[s]" must "refrain from disclosing the nature or details of services provided to patients." 410 ILCS 50/3.

99. Under 735 ILCS 5/8-802, "[n]o physician or surgeon shall be permitted to disclose any information he or she may have acquired in attending any patient in a professional character."

100. Advocate may also not disclose personally identifiable information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

101. Plaintiff and Class members performed all required conditions of their implied contracts with Advocate.

102. Advocate breached the implied duty of confidentiality to Plaintiff and Class members by intentionally deploying tracking pixels and web beacons on its LiveWell portal that caused the transmission of personally identifiable patient information, PHI, and communications to third parties, including Facebook.

103. Plaintiff seeks all monetary and non-monetary relief allowed by law.

FIFTH CAUSE OF ACTION

Invasion of Privacy - Intrusion Upon Seclusion
Advocate Defendant

104. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

105. Plaintiff's and Class members' communications with Advocate constitute private conversations, communications, and information.

106. Plaintiff and Class members have a reasonable expectation that Advocate would not disclose personally identifiable patient information, PHI, and communications to third parties without Plaintiff's or the Class members' authorization, consent, or knowledge.

107. As a healthcare provider, Advocate has a duty to keep personally identifiable patient information, PHI, and communications confidential.

108. Advocate expressly promises to keep patient information secure and to take "steps that are designed to make all information received from our LiveWell subscribers as secure as possible and protect against unauthorized access and use."[10]

109. Advocate intruded upon Plaintiff's and Class members' seclusion by deploying tracking pixels and web beacons that caused the transmission of Plaintiff's and Class members' personally identifiable patient information, PHI, and the contents of communication Plaintiff and Class members exchanged with their healthcare providers to third parties, including Facebook.

110. Plaintiff and Class members did not authorize, consent, know about, or take any action to indicate consent to Advocate's conduct alleged herein.

111. Plaintiff and Class members' personally identifiable patient information, PHI, and communications are the type of sensitive, personal information that one normally expects will be protected from disclosure to unauthorized parties by the very entity charged with protecting it. Further, the public has no legitimate concern in Plaintiff's and Class members' personally identifiable patient information, PHI, and communications, and such information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

[10] *See* https://www.advocateaurorahealth.org/livewell/privacy.

112. Advocate's conduct described herein was intentional and highly offensive to a reasonable person.

113. Advocate's willful and reckless conduct in allowing access to and disclosure of Plaintiff's and Class members' sensitive, personally identifiable patient information, PHI, and communications to unauthorized third parties is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

114. Due to the invasion of privacy caused by Advocate, Plaintiff and Class members suffered and will continue to suffer damages and injury as set forth herein.

115. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

PRAYER FOR RELIEF

Wherefore, Plaintiff Alistair Stewart respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Alistair Stewart as Class Representative, and appointing Stephan Zouras, LLP as Class Counsel;

B. Declaring that Advocate and Facebook's actions, as set forth above, violate the ECPA, 18 U.S.C. § 2511 (1)(a), (c)-(d);

C. Awarding statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000 to Plaintiff and each Class member, as provided by the ECPA, 18 U.S.C. § 2520(c)(2);

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding Plaintiff and the Class their reasonable attorneys' fees and other litigation expenses, 18 U.S.C. § 2520(b)(3);

F. Declaring that Facebook's actions, as set forth above, violate the SCA, 18 U.S.C § 2701(a) and constitute a breach of contract;

G. Awarding statutory damages of the sum of the actual damages suffered by the Plaintiff and Class members and any profits made by Facebook as a result of the violation, no less than $1,000, 18 U.S.C. § 2707(c);

H. Declaring that Advocate's actions, as set forth above, constitute invasions of the implied duty of confidentiality and invasions of privacy as defined by Illinois law;

I. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Plaintiff and the Class;

J. Awarding Plaintiff and the Class their reasonable attorneys' fees and other litigation expenses, 18 U.S.C § 2707 (b)(3);

K. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable;

L. Awarding such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Date: October 28, 2022

Respectfully Submitted,

/s/ Ryan F. Stephan

Ryan F. Stephan
James B. Zouras
Teresa M. Becvar
Mohammed A. Rathur
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza, Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
rstephan@stephanzouras.com
jzouras@stephanzouras.com
tbecvar@stephanzouras.com
mrathur@stephanzouras.com
Firm ID: 43734

ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on October 28, 2022, I filed the attached with the Clerk of the Court using the ECF system which will send such filing to all attorneys of record.

/s/ Ryan F. Stephan